

CIO Council Meeting Minutes
June 25, 2003
Commission Room
Administration Building

Attendees: Gary Alexander, George Bakolia, Randy Barnes, Julie Batchelor, Cynthia Beck, Bob Brinson, Mary Sue Brown, Ann Brown, Fletcher Clay, Amy Edwards, Mike Fenton, Charles Fraley, Bruce Garner, Ann Garrett, Mary Jo Gilliam, Elaine Glass, Janice Hodges, Christopher Houghland, Steven Hulse, Mark Hughes, Ed Johnson, Angela Jones, Ron Kennedy, Wendy Kuhn, Bill Kurdys, Cliff Layman, Joe Lithgo, Smitty Locklear, Nancy Lowe, Lee Mandell, Ben McLawhorn, Don Nattress, Julia Nipper, Tony Schiro, John Twomey, Bill Wade

Chairman Locklear called the meeting to order at 10:00 a.m. Announced Angela Jones as monthly scribe and introduced Mary Joe Gilliam, Department of Agriculture.

MINUTES: The minutes of the May meeting were approved without correction.

ELECTIONS: Smitty announced that Gary Zeller won the election as Chair and motion to approve was made and second. The election of Vice Chair was tied between Randy Barnes and Cliff Layman and would be decided by ballot at this meeting. Elections were held via ballot and the outcome was still a tie 7/7. Randy Barnes withdrew her nomination and Cliff Layman was named the new Vice Chair. In addition, there will be 3 board members leaving. Smitty plans to meet with new chair in reference to voting via email. CIO members agreed to vote using email.

IRMC Updates

Not much to report. Woody thanks everyone for your continuing support of the WF school project. August IRMC meeting has been cancelled. A new date has not yet been set.

SECURITY

1. Security Gap Analysis Project Update

I am pleased to report that the first phase of the IRMC/IPPC sponsored security initiative is complete. The findings and recommendations from the Gap Analysis of Security Policy, Standards, Procedures and Architecture are now in the review cycle and Katherine White of the ITS Security Office sent you a copy of the Executive Summary of the report. As you know, in this first phase, the chosen vendor CIBER performed a gap analysis to evaluate current statewide security policy, standards and procedures and the security technical architecture as compared to industry standards and legal and regulatory requirements. The vendor also conducted a series of interviews with members of various groups such as the IPPC, ITMAC, CIOC, the universities, CJIN and agency security liaisons to better ascertain the current status and requirements for security policies, standards, procedures and the architecture.

In addition to the gap analysis, the vendor suggested priorities and drafted a work plan for implementing and maintaining the required set of policies, standards and procedures at both the state and agency levels. The estimated hours of effort can be used to determine the cost (+/- \$1 million) to create the required items, keep them current, and to train the agencies.

The vendor presented the deliverables to the IPPC steering committee members at their meeting on 6/16 and then presented the results to the agency security liaisons and other agency stakeholders on 6/17.

PROJECT FINDINGS:

- Existing policies, standards, and IRMC approved documents offer excellent content material for the creation and/or expansion of additional policies and standards.
- The secure portal is an excellent resource.
- Credit should also be given to the supporting information security infrastructure evidenced by the enabling legislation, IRMC, IPPC, Security Liaisons, the State CIO and CISO, and numerous State employees that support and provide input for the improvement of information security.
- The Statewide Technical Security Architecture (Chapter 12 of the Statewide Technical Architecture) provides an excellent source of security information relating to specific technical controls and their employment.
- The existing zoning standard provides a good basis for establishing appropriate levels/layers of security and defining a zoned security architecture.

PROJECT RECOMMENDATIONS:

Current Action Items:

- Endorse the study and use the priorities.
- Approve the recommended frameworks for the Statewide PSPs and the Technical Security Architecture
- Develop a Request for Comment (RFC) approach where the proposed policy, standard, procedure or architecture is posted in a common location at a specified time for a prescribed comment period. After the prescribed comment period, the author would draft a response, modify the document accordingly, and circulate it to reviewing committees who would then act on the original, the comments, and the revision.
- Adopt and use the Glossary of Information Security Terms. (A draft of the glossary has already been sent to you.)

Identify Funding to Complete the Recommendations:

- Fill in the gaps. Gaps exist between the current PSPs and TSA and the proposed PSPs and TSA frameworks. All identified gaps are correctable. The State has good content and recommended plans to accomplish this formidable task.
- Train agency staff on both policy development and technical architecture and on the implementation and maintenance of both.

I want to thank all of you for your help and support with this effort and ask for your continued support in implementing these results.

2. Agency Security Assessment

The responses to the scope statement for the second phase of the IRMC/IPPC sponsored security initiative were received on 6/16/03. They are being reviewed and a vendor should be selected soon to set up the project office. The selected vendor will be tasked with developing, implementing, staffing, and operating a project office for conducting a statewide security assessment effort. This project office model is based on the Y2K model.

LEGISLATION

I am pleased to report that Governor Easley has signed two significant bills dealing with information technology.

These two bills represent major steps in our efforts to improve security and to save taxpayers' money by delivering services more efficiently. The involvement of the CIO Council will be crucial in implementing these two pieces of legislation.

1. IT Legacy Study

House Bill 941 authorizes the Office of Information Technology Services, in conjunction with the IRMC, to study the state's legacy systems.

Specifically, the legislation requires ITS to analyze the state's legacy systems and develop a plan to ascertain the needs, costs and time frame required for state agencies to move to more modern systems.

A report on the **assessment phase** of the analysis is due to the Joint Legislative Commission on Governmental Operations by **March 1, 2004**. In subsequent years, ITS is required to make an annual report to the Commission by March 1. In order to get the assessment completed on time, we will have to begin this work shortly. I welcome any suggestions that you have for getting started.

After the assessment phase, ITS is authorized to determine the **needs, costs and amount of time** that would be required to modernize State agency information technology. This portion of the study must be completed by **January 31, 2005**, with a report to the 2005 General Assembly. ITS will update that report every two years.

2. IT Gap Analysis and Security Changes

HB 1003 combined two measures into a comprehensive bill that addresses security on two fronts.

First, as you've already heard, it authorizes the state CIO to conduct an agency-by-agency assessment of compliance with the current, enterprise-wide set of security standards.

The study will include an estimate of the costs to implement the security measures that would be required to fully comply with the standards.

The bill also includes provisions beefing up the state laws dealing with IT security.

Under the measure, agencies must report all security incidents within 24 hours of confirmation.

Agency IT liaisons will be subject to criminal background reports, and agencies will be required to develop and continually review and update a business and disaster recovery plan. Those plans will be submitted annually to me and to the IRMC.

Reps. Tolson and Paul Miller and Sen. Eric Reeves were the primary sponsors of this legislation, and they should be commended.

OPERATIONS

1. **State Portal Migration:** ITS began hosting the State Portal on June 14, two weeks ahead of schedule. As part of this migration, ITS has enhanced the redundancy and security of the State portal hosting infrastructure. This migration was the result of effective cross-functional collaboration between Enterprise Solutions, Computing Services, Telecommunications Services, Customer and Public Relationship Management and the Information Security Office.
2. For the month of May the **Common Payment Service** processed over 107,000 credit card and ACH transactions worth a total of \$56.5 million.
3. **IPX-IP Migration:** DOT plans to complete their phase one migration on June 26. ITS will then make the final LAN Directory changes to complete phase one. Phase two is underway. All 32 affected agencies have submitted their phase two plans. Eight agencies have completed their phase two migration. Detailed phase two migration assessment and follow-up is in progress and a schedule is being developed.
4. **Storage User's Group:** Agencies have responded well to ITS' Storage Users Group. So far the meetings are well attended and have generated positive feedback. The Storage Users Group is intended to foster more efficient storage management practices across agencies and to encourage and educate agencies in the use of more efficient storage management practices. Interested agencies should contact ITS' Computing Services Director, Ross Yannayon, at 981-5100.
5. **Implementation of Trust Zone Hosting:**
 - ITS Trust Zones are operational
 - Initial migrations of Computing Services systems management consoles and NC Portal are complete
 - Mainframe Test LPAR was migrated on June 22
 - Mainframe production LPARs scheduled to migrate by 7/27/03
 - ITS LAN migration will follow (4-6 weeks).
6. **Linux on the Mainframe:** As we have previously reported, Computing Services is migrating static web sites to Linux on the Mainframe. CS continues with analysis and prioritization of web site migrations, which will likely be completed in August.

ListServ/Majordomo Service

Low complexity, low cost, short time to implement

Overview

Internet mailing lists (ListServ/Majordomo) expand the functionality of LAN-based or host-based distribution lists by providing the capability to send messages to a single Internet email address and having that single address represent an entire list of email addresses across the Internet. By using standard techniques for sending mail, it is a simple and transparent process to the sender. The computer which runs the list holds the responsibility for distributing messages to all addresses on the list. Email users send electronic mail messages addressed to the list that the server will forward to all other members of the list. This service provides a convenient means for the exchange of ideas and information between list members. There can be many different lists with each of them containing users who share particular interests (communities of interest).

ITS has implemented ListServ/Majordomo services on a Unix host as a method of creating and establishing Internet mailing lists. Once a list is created, anyone can send email to the list name but it would be recommended that lists be focused on "communities of interest" in an attempt to focus the e-mail correspondence to the people that have indicated an interest in the list(s) they have subscribed to.

ITS can create an Internet mailing list for any NC public agency upon request. The list can be created with the subscription policy configured as "closed" - which means all subscriptions to the list must be approved by a list owner or moderator. The client would designate at least one person to be the list owner. It is recommended that two people (primary and a backup) serve this function in order to avoid any delays in handling administrative functions of the list. The cost for maintaining any given list is \$25/month per list. The use of this service is designed for NC public agencies only and not for general use outside of NC state government. George Bakolia reported that the \$25 per month fee could be waived as long as the system is being used.

A CIOC process would have to be in place. A scope would have to be defined to decide how many lists would be created. George Bakolia asked that more CIO members get involved because the decisions made will effect their staff.

File Attachment Issues with ListServ Option

You can use attachments effectively within this service if they are "text" based files. You could also just cut and paste the "text" right into the message itself. ListServ can handle text file attachments or embedded text just fine but problems can occur when you attach a file that is in some type of proprietary format (such as WORD, Powerpoint, etc...).

The ListServ/Majordomo function has an inability to consistently retain the attributes for the contents of these types of files. E-mail systems have been specifically designed to handle this challenge but ListServ capabilities have not. There are some alternatives to working around this issue - none of them are particularly elegant - that I would submit for your consideration :

If the attachment content can not be converted to text format for embedding within the message or as a text file attachment, then :

1. You could post the file to a shared web site (the location of which is determined ahead of time) and the originator of the ListServ message could include a URL link in the ListServ message to that specific file at the URL location indicated. Anyone who wanted/needed this file could gain access to the file (security permitting of course) via the URL link.
2. The originator could simply indicate in the ListServ message that if anyone would like a soft copy of the file referenced in the ListServ message, that they could request a copy directly from the originator via their personal e-mail address and the originator could e-mail the soft copy directly to the requester.

The issue of attached files retaining their specific attributes has long been an issue with ListServ's. It was never designed to deal with such things which is why e-mail systems & solutions have evolved the way they have.

Project Management Classifications

Randy Barnes provided handouts of the presentation that was given to CIO Planning Committee that includes a summary of where the project stands.

Why project management? Specialization and the unique skills. Failure of IT projects is rarely attributable to just technical shortfalls. It projects require pulling many diverse organizations together toward a common objective.

Why do we need specialized positions? Expectations are higher from customers, staff, management and vendors. Technology is the cornerstone of nearly every service delivered by the state. Appropriate positions will allow us to attract and retain key skill sets necessary to establish and maintain a strong IT environment in NC – today's market makes it harder to retain.

Portfolio management is necessary for a clear understanding of agency goals and prioritization of needs such that resources are deployed to gain the most value – right things in the right order.

Increased emphasis on Project Management. No longer associated with just applications development efforts. Technology needs a complex set of skills to manage. Key factor in the success or failure of large automation projects is the adherence to project management industry standards. Requires diverse technical knowledge. Requires people and business skills.

The primary goal of a PMO is to ensure that a program achieves its business objectives.

Benefits. Help to infuse the Project Management discipline in to the agencies. Expand expertise; help reduce the dependency on outside resources. Improve morale.

Project management status:

Presented to CIOC planning committee on 6/18/03.

Presented to Don Nattress (OSP) on 6/1/03

Next Steps:

Provide OSP with recommended criteria to differentiate progression between levels.

Provide OSP with suggested leveling recommendations.

Subcommittee plans to continue on and ask for feedback. Once classifications are in place training should be established. It was suggested that the subcommittee contact other states that already have this in place and ask for their input.

Randy thanked Mr. Nattress for his support and willingness to work with the committee.

Project Certification Approach (Update)

Mike & Woody are moving forward with process. It is just in the beginning phases and is not complete. The negotiation of a new certification process, #1 streamline the process. #2 Needs IRMC to do oversight - needs more time to look at needs and compile input.

This is in draft format at this time and waiting for further input. Several members expressed frustration. There is a feeling that some of the real issues are not being addressed and others because they submitted input and had no feedback given. Mike agreed that communication is a problem. Mike further agreed to brief Janice and make her aware of the problems.

In closing Smitty expressed his pleasure to serve as the chairperson for the past 2 years. He appreciates all the members trust and support and ask they support Gary in getting his job done.

Meeting adjourned at 12:05 p.m.